Aaron Allan

Partner, Glaser Weil

aallan@glaserweil.com
irglobal.com/advisor/aaron-p-allan
+1 310 282 6279

Aaron P. Allan, a Senior Partner in Glaser Weil's Environmental & Energy Department, has for more than two decades litigated cutting edge and "bet the company" cases for a diverse range of business entities, including significant environmental and insurance coverage cases, toxic tort cases and real property litigation matters.

Mr. Allan has long represented water utilities accused of delivering contaminated drinking water and many other companies subjected to claims brought under CERCLA and other environmental laws.

Alexander J. Suarez

Associate, Glaser Weil

asuarez@glaserweil.com
glaserweil.com/attorneys/alexander-suarez
+1 310 282 6279

Glaser Weil Associate Alexander Suarez specialises in commercial disputes and business litigation. He represents clients in complex commercial litigation involving insurance recovery issues, financial services, and real estate.

Mr. Suarez is experienced in all phases of litigation, from filing and answering complaints, through discovery, trial, and appeals. He has trial experience in both California state and federal courts and also has experience in arbitration.

glaserweil.com

I QUESTION ONE – CHALLENGES

What do you see as the biggest challenges for data privacy in your jurisdiction during the next decade? Is technology a factor?

The biggest challenge for data privacy in California will be the implementation of (and compliance with) the California Consumer Privacy Act (CCPA), effective January 1, 2020, which is the most comprehensive consumer privacy protection law in the United States. Like the GDPR, the CCPA has caused considerable uncertainty and concern, particularly given the potential for significant civil penalties, underscoring the importance of compliance. Fortunately, the California Department of Justice recently proposed regulations providing guidance on compliance with the CCPA.

For example, the CCPA obligates subject businesses to notify consumers of the categories of personal information they collect and the reasons for its collection, at or before the time it is collected; it does not say how businesses must satisfy that obligation. The proposed regulations specify that the requisite notice must be in plain language, legible, available in languages that the business uses in transactions with consumers in the ordinary course, accessible to consumers with disabilities, and visible or accessible to consumers before the collection of their personal information. The proposed regulations also provide examples of how businesses can make the disclosure online (e.g., by posting links to the notice on pages where information is collected) and offline (i.e., by giving notice on forms and via conspicuous signage). Businesses wondering what they must do to comply with the CCPA should consult with legal counsel or look to the implementing regulations for more specific guidance.

I QUESTION TWO – ENFORCEMENT

How is enforcement of data privacy breaches keeping up with the rapidly changing regulatory environment. What are the trends you are seeing in your jurisdiction?

California has shifted toward consumer empowerment in data privacy enforcement. The legislative history of the CCPA shows the Legislature recognised the enormous value of consumer data, and drafted the act with the express purpose of giving consumers greater control over their personal information. The Senate Judiciary Committee's August 31, 2018 Bill Analysis observes: "The world's most valuable resource is no longer oil, but data" and "[w]ith [the] widespread collection of data comes serious concerns about consumers' privacy." The Analysis affirms that the CCPA's "goal was to empower consumers to find out what information businesses were collecting on them and give them the choice to tell businesses to stop selling their personal information" and to provide "a modified enforcement mechanism to protect those rights."

Even in the absence of a data breach, the CCPA empowers a consumer to request that a business subject to the act:

- disclose the categories and specific pieces of personal information about the consumer collected or sold;
- delete personal information that the business collected from the consumer;
- disclose types of personal information about the consumer sold to third parties, and describe the categories of third parties to whom the information was sold; and

- not sell the consumer's personal information to third parties.

The CCPA is primarily enforced by the Attorney General but it also provides for a limited private right of action for consumers whose "nonencrypted or nonredacted personal information" is subject to "unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures."

If the consumer gives the company written notice specifying which provisions of the CCPA it violated and if those violations are not cured within 30 days, the consumer may sue, on an individual or class-wide basis, for statutory damages of between $100-750 per consumer, per incident or for actual damages, whichever is greater.

QUESTION THREE – UNIFICATION

The European Union's General Data Protection Regulation (GDPR) was the big data privacy story of 2018. What has been the impact of this in your jurisdiction and are you now seeing greater efforts at international cooperation?

On September 24, 2019, the European Court of Justice ("ECJ") decided Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), and in the process construed Article 17 of the GDPR. Article 17 allows individuals in European Union Member States to request that their personal data be erased in certain circumstances, for example, where the person objects to the processing of his or her personal data on certain grounds and the data controller does not demonstrate "compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims." This has also been referred to as the "right to be forgotten."

In Google LLC, the CNIL demanded, in response to a request for erasure under Article 17, that Google remove information subject to the request globally, and not just from results for searches conducted within EU Member States. Google refused, removing the information subject to a request for erasure only from results for searches conducted within EU Member States. The ECJ's preliminary decision was in favour of Google's interpretation of the right to be forgotten. As a result, Google can make information subject to a GDPR request for erasure available outside of EU Member States.

The decision calls into question whether the GDPR will drive greater efforts at international cooperation in data privacy and information security. The ECJ's ruling was very important to tech firms in Silicon Valley, particularly internet search providers and social media companies. The ruling makes clear that the right of erasure requires only that the information subject to a GDPR request for erasure be made inaccessible in EU Member States, but may nevertheless be made accessible in non-member states. It is worth noting, however, that the CCPA mirrors many of the GDPR's consumer protections, exceeding them in certain respects.

Data Privacy in California

1. Get ready for California Consumer Privacy Act (CCPA) compliance. On January 1, 2020, consumers will have the right to request personal information about them collected or sold by a business during the preceding 12 months.
2. Ensure ongoing compliance with federal, state, or local laws governing data privacy. These laws are not impacted by the CCPA.
3. Keep current with cyber-insurance coverage. Given the potentially devastating costs of a data breach, businesses must keep current with the rapidly evolving landscape of cyber-insurance coverage.
4. Develop a data breach response plan and practice its implementation. An actual data breach should not be the first test of your response plan.
5. Take a multi-jurisdictional approach to data privacy compliance. For example, compliance in California may not satisfy obligations under the EU's General Data Protection Regulation (GDPR).